Rocks and Shoals

Navigating Incident Response

Smooth Sailing Solutions

Gen. Dwight D. Eisenhower, 1943.

National Archives (63-92)

MVIR01-1.0 08 January 2020

smoothsailingsolutions.com

1 Introduction: Incident Response

> [P]lans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of "emergency" is that it is unexpected, therefore it is not going to happen the way you are planning.
>
> Dwight D. Eisenhower, 1957

There's an old saying that goes, "anything that will not kill you in the next thirty seconds is not a crisis–it's a situation." The point of this is to remind us that as conscious individuals, we can control our destiny to some extent, respond to events, and influence–if not control–the fallout of the things that happen around us.

The same is true for businesses and other organizations in that we can't prevent various incidents from occurring, but it is possible to control how we respond.

Generally speaking, that's what Incident Response is all about: identifying incidents, practicing your responses, keeping things moving. But the details are complicated.

The trouble is, when we talk about incident response and particularly building out incident response programs, the focus is often on the "plan". Most organizations have response plans of various kinds–what to do in the event of a fire, or a power outage, or an earthquake. And by calling them *plans*, we give credence to the idea that the point of incident response is to prepare for incidents so we can know what to do when they happen.

Which is just not how this works.

This is not to say we shouldn't do planning and preparation. They're essential activities, but the goal is not to develop a plan. The goal is to go through the process of thinking about a situation and building relationships and familiarity with the resources needed to respond. In other words, the goal is to be thoroughly familiar with the practice of thinking through problems and responses, so that when an incident happens, you're ready to create a plan and carry it out.

Create the plan as part of the incident response, not before the incident.

Plans include assumptions. Assumptions like who will be available to respond to the incident, the nature of the emergency, the resources affected or available at the time. And those assumptions are all, of necessity, completely invalid. If you could predict with any accuracy what the situation would be like, that's not an incident response; that's a project.

So let's talk about what incident response looks like.

1.1 Glossary

The language we use to talk about incident response and preparation is sometimes a sticking point, so it's worth spending some time to make sure the words we use here mean the same thing to everyone.

This is by no means an exhaustive list, but it's a good starting place not only for reading this document but also for making sure your audience is on board when you start talking about these concepts.

After-Action Report: A set of documents and associated analysis identifying the causes and attempted responses to incidents. Effective After-Action Reports focus on possible mitigation and prevention measures to be implemented, and they avoid assigning blame or “litigating” responsibility for issues.

Incident: An event that disrupts or threatens to disrupt the normal operation of an organization.

Incident Response: Activities intended to repair the disruption caused by an incident. Incident Response includes all work done in preparation for incidents, not just the work done following an incident.

Plan: A set of expected actions, activities, or procedures to be completed in pursuit of a goal. In Incident Response, plans are often created but rarely followed.

Risk: The probable frequency and the magnitude of a future loss. You’ll often see this simplified as “probability times impact equals risk”.

Risk Management: A program or process by which risks are evaluated, prioritized, and managed by an organization.

See *Rocks and Shoals: Navigating Risk Management* for an example of an effective Minimum Viable Risk Management Program.

Scenario: An incident created for the purpose of conducting exercises. Complete scenarios include not only actions and events, but context and limitations simulating the complexity of real world events.

Wombat: A short-legged, muscular burrowing Australian marsupial of the family *Vombatidae* resembling a small bear. Wombats are affable and darn cute.

2 The Basic Plan

The *Minimum Viable Incident Response* program is implemented by following these steps:

1. Assemble the team,
2. Define priorities,
3. Create a response plan,
4. Fix your response plan,
5. Measure your progress,
6. Test your team,
7. Executive review and approval,
8. Document and review program results.

2.1 Assemble the Team

So, plans aren't that helpful because incidents don't follow the plan–your organization needs the ability to think and react, to use uncertain information and assets to achieve goals you can't predict. The only answer to that problem is to use people.

In fact, you need a lot of people. People with a range of skills who are capable of adapting to situations as needed. People who can work together. People who can work independently. People who can work with complete strangers.

Here's the big secret of this step–you're not assembling a team of people to handle incidents. You're building a team of people to make your organization resilient and able to respond to incidents. That's a very different job, and a very difficult one–it would be a lot easier if you could just create a team of superheroes to handle the problems. Unfortunately, that remains the domain of comic books.

So, a team to make your organization more resilient. That's going to vary depending on the size of your organization and how complex your needs are, but you need people in each of these roles:

- Executive management. One or more members of the top people in the organization, who can make policy and enforce it as needed.
- Production experts. Whatever services or products your organization provides, you need people who thoroughly understand how that happens and the critical pieces to put it together. Think about program managers, directors, and so on, but also engineers and front-line workers.
- Procurement. Who buys the components and coordinates the vendors on which you depend? For that matter, who could quickly arrange for budget resources to bring in supplies or replacements?
- Marketing and Sales. The most commonly overlooked function in incident response is communication with your customers and partners. It doesn't matter how good you are at restoring service after an incident if you can't effectively communicate what happened and how you responded.
- Legal. Someone needs to be thinking about long-term consequences and remediation, even if it doesn't make sense in the short term. Many highly effective response teams have ended up creating severe problems for their organizations because no one recognized their actions were opening new liability risks. It's sometimes necessary to take those risks, but there needs to be someone keeping track and thinking about the long-term remediation and cleanup.

In all of these roles, look for people that are respected by their peers. In particular, pay close attention to the so-called “soft skills”: people who can communicate effectively and empathize and work with others who have a different point of view, and people from a variety of backgrounds. Your organization should be well-represented not just in the roles your team members fill, but in the kinds of people who make your organization what it is.

2.2 Define Priorities

Incidents are messy, which means the response is often messy, too. Deciding on a course of action, or even choosing which of several immediate issues to tackle first, is often a game of picking the least-bad option. Sometimes even that isn’t clear.

In those moments, it’s helpful to have a predefined list of priorities and goals. The top of the list is generally simple–protect the lives and health of any or all personnel or bystanders. But then what? Is the equipment for future production more or less valuable than current usable inventory? Is maintenance of information security controls around sensitive information critical before restoring service to customers, or should it be a follow-up item?

The goal is to build a simple, straightforward list of priorities that anyone in the organization can see and understand so that during incident response, those facing difficult choices have applicable guidelines no matter what the details might be. To start, use this basic list and discuss how its rankings apply and whether or not they’re appropriate; update and add to it as needed, based on the results of both simulated and real incidents.

1. **Health and safety of people, including employees, customers, and bystanders.** With rare exceptions, there's no value in ranking or prioritizing groups of people. Your employees should not be more valuable than customers, or vice versa, customers should not be more valuable than bystanders, and so on.

2. **Environmental impact on communities, ecosystems, and habitats.** This one generates some controversy, but it's an important consideration and one that's often overlooked. Particularly in the context of modern sensitivities to environmental harm and climate change, failing to assign a priority here is, at minimum, likely to lead to a public relations impact, if not a regulatory and financial one.

3. **Future production capacity and long-term organizational health.** Your organization's ability to function and provide services later is more important than eliminating downtime. You most often see this issue in online service providers and physical plant operations– people use the urgency of alarms and outages to skip testing steps in getting back online. Yet this often creates more significant issues when systems stressed by the initial incident aren't properly repaired before resuming operations, which prolongs incidents and creates much larger impacts.

4. **Evidence for post-incident investigation.** If the incident was or likely could be the result of malicious activity, evidence of that activity may be destroyed in a rush to bring services back online. Think about how your normal operations might impact this evidence, how you could preserve it, and decide now whether you should prioritize preservation of evidence over short-term revenue losses.

5. **Short-term revenue impact to the organization.** Health and safety plus environmental factors considered; future production capacity secured; okay, now it's time to do what you can to protect or preserve the current inventory or service capacity. In the moment, this often seems to be of paramount importance; over the last few decades, companies have invested a lot of time and energy on productivity and assigning dollar values to all kinds of activity and outages. The reality, however, is that the cost of returning to service too quickly or failing to consider the impact on staff, public relations, or your organization's ability to maintain service often outweigh the short-term benefits of reducing losses.
6. **Economic impacts on third parties.** No business operating today is independent of every other company; we all have partners, service providers, vendors, or suppliers who may be affected. Those companies have owners and employees and representatives who will often have a voice within your organization. The impacts of your incident response on those organizations shouldn't be ignored, but they also probably shouldn't take precedence over other considerations.

As you read through these priorities, you may well disagree with them, or think of other things that should be listed. That's great! The goal is not to persuade you that these priorities are the correct ones–it's to get you thinking about what the priorities are for your organization.

And don't forget to *write them down* and make sure people know about them.

2.3 Create a Response Plan

I know. I know! We just said plans are worthless in incident response, and now here we are in step three telling you to make a plan. But it's important, it really is.

You see, plans are worthless (or at least, not very valuable). *But the process of creating a plan is extremely helpful.* It's a great way to get people thinking and talking about the problems you might face. When they have those conversations, the information and the reminders will be useful later on during actual incident response.

In November of 1969, Apollo 12 launched from Florida en route to the Moon. Just a few seconds after liftoff, lightning struck the spacecraft–twice. The lightning caused a huge number of problems and issues, some of which persisted throughout the mission. But the most critical problem from the perspective of the launch controllers and teams supporting the mission was that all the telemetry from the spacecraft went away, and then didn't restore itself to anything useful–it was all garbage.

In the middle of trying to figure out what was going on, 24-year-old John Aaron made a now-famous recommendation–"Flight, try SCE to Aux". Alan Bean, the Lunar Module Pilot, heard the call and made the change, data flowed, and the rest is history.

But here's the point I want you to remember about this story–"SCE to Aux" was not a standard procedure anywhere for this problem. It wasn't (as is often reported) something Aaron had seen in an earlier electrical failure simulation, either. He made the recommendation based on gut feel and a solid understanding of the various systems and their interconnections.

Your First Response Plan

It almost doesn't matter what your first response plan looks like, as long as it involves getting people talking about how your organization should respond to an incident. One of my favorite places to start is with an incident response plan we all need but haven't put much effort into.

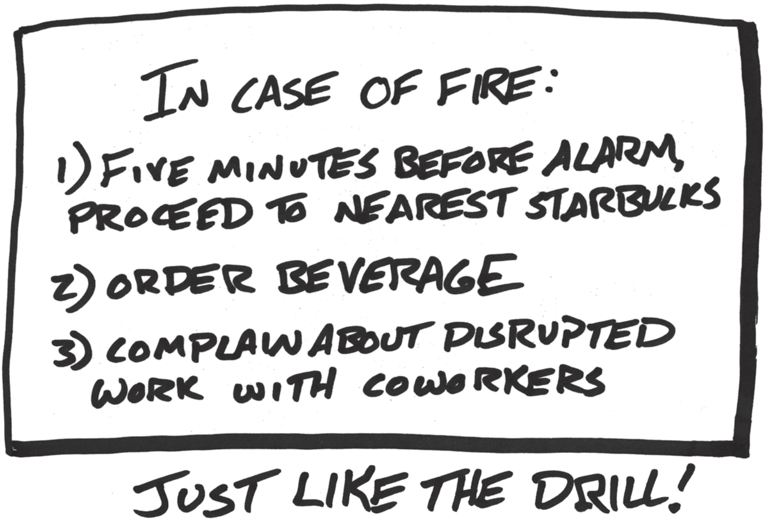
That's your fire evacuation plan.

A typical fire drill involves a lot of compromises. People know it's coming, so many of them schedule off-site meetings or work from home on the day of the drill. Safety wardens and others are prepped and pre-positioned for the drill.

Often, plans are implicitly or explicitly built on the assumption that everyone is fully mobile and capable of evacuating under their own power. Any one of these issues would be enough to make the "plan" unworkable, and many organizations have all of them.

Which of those issues apply to your company's fire drills?

How would you fix it? What would make your evacuation plan more useful, and how would you get your staff on board with it?


IN CASE OF FIRE:
1) FIVE MINUTES BEFORE ALARM, PROCEED TO NEAREST STARBUCKS
2) ORDER BEVERAGE
3) COMPLAIN ABOUT DISRUPTED WORK WITH COWORKERS
JUST LIKE THE DRILL!

Knowing that the mission would be aborted if the problem wasn't solved immediately, he guessed from outside the predicted options. The flight director knew and trusted his team, so the change was made within seconds.

All of which is the direct result of hundreds of hours of training and simulations, involving the flight controllers, crew, and the teams supporting them. The plans they created ended up being mostly useless. In hindsight, it might seem obvious that lightning could strike and create problems, but it wasn't in the books on that November day. However, the process of creating those plans was invaluable because it enabled the full team to effectively respond to an unexpected incident and save the mission from abort or disaster.

So… plans are not the point. But going through the planning process is an essential step in building the kind of team that can handle incidents calmly, efficiently, and successfully.

2.4 Fix your Response Plan

The planning process is critical to building a resilient, incident-responsive organization, but you build the plan with a subset of the organization. This is the time to find out what you need to adjust in your team.

Start by publicizing the work as often as possible, and solicit feedback and engagement from the entire organization. Publish the result; consider the possibility of a large-group presentation to the company. An all-hands meeting or retreat is an excellent opportunity to solicit feedback and check in on how people are thinking about incident response.

One thing, though–if you decide to go that route, avoid scary scenarios for the presentation. Choose something unlikely to provoke traumatic responses or be depressing. I like to use "wombats have escaped a nearby zoo and are disrupting operations by being adorable in common areas."

Take the information and feedback you get from this process and use it to improve the program. Did the larger audience find issues you didn't consider?

Think about what those issues suggest about the perspectives of your planning team. Do you need to add more people, or would different representatives be a better option, or should you just use the opportunities to engage more teams outside of the planning group?

Is the overall group interested and engaged in what you're doing and how it affects their work? If not, what can you do to engage them? How do you build awareness of your program and its benefits?

2.5 Measure Your Progress

This is a great time to talk about measuring process and success. By default, most programs are measured by their plans–how many they've created, the successful tests they've run, and so on. But as we've said throughout, the plan is not the goal, and it's not even a particularly valuable part of the program.

At the same time, any new initiative or program needs some way to measure results and report back to management. So if it's not going to be the publication of incident response plans, what should it be?

Program Products

The Response Plans might not be valuable in themselves, but that doesn't mean the team doesn't produce anything. As you go through the planning process, you'll identify things that you need to do–risks that haven't been mitigated, supplies that aren't readily available, and processes or company activities that no one's documented.

The team should work to address those issues, and as they do, track and record the activity. There's no hard and fast rule for how much activity your program should generate, but as it changes over time, it gives you indicators of your program's health. Does activity pick up when you implement new production plans or change facilities? Does it taper off when things are relatively stable? Look at the quality of the activities, too–it's easy to look busy by asking for lots of information, but pay attention to recommendations for changes and scenarios as those requests are answered.

And if people aren't answering the requests for information, well, that tells you important things too.

Engagement

Are people in your organization paying attention to your program's efforts and results? Do you get questions about incident response from outside the team? Are people reading the updates and recommendations your group provides? Do people find your team and its activities helpful, boring, or annoying?

Actual Effectiveness

It would be lovely if incidents remained theoretical exercises to think about. But sadly, into every company's operations, a little rain must fall. So how does your company do? Hopefully, you don't have too many incidents, but pay attention and track them–not just the ones your team is directly involved in, either. One simple example: your IT help desk will probably be heavily involved in most incidents, either directly or in helping communicate issues and collecting information. Which means they're going to be an early participant in your program.

What happens to their reporting metrics after working with your team? Do they respond better, faster, more effectively? Don't take all the credit, but if their metrics improve as a result of working with you, that's worth a hundred binders of incident response plans.

2.6 Test Your Team

So you've built a team, created some incident response plans, and used them to make changes to your organization. You're paying attention to how things are going, and it seems like your team has positive effects.

Now what?

Now, it's time for the fun part.

Incident response testing is everyone's favorite part of incident response. You get to make up scenarios and try to overcome them; it's like a role-playing game. You can even use dice and game boards if you like. Once you've got your team up and running, you should be running regular incident response scenarios–usually quarterly. Pick real scenarios when you can, using incident reports and examples from the news. Assemble a team of people to go through the exercise, and walk through all the steps; how would you respond? What would the likely results be? How does that compare to what actually happened and their results?

When you do this, though, there are some common pitfalls many organizations run into. Do your best to avoid them to make your program an effective one.

Don't Depend On Your Core Team

It's tempting just to use your planning team for the incident response simulations. They know what's at stake, they understand what's going on, they're relatively easy to schedule. Which is also a good list of reasons why you shouldn't use them.

Real incidents, of course, don't go according to plan. They happen at midnight, they come when half your team's on vacation, and they drop in the laps of people who've never been part of your team and have to be handled before anyone else can take over. Which means you can't count on controlling who's going to be involved when an incident happens, or on them being prepared.

Solicit the involvement of people from outside your team. Ideally, your team should be observers–what do people try, or think of, that wouldn't occur to the team? Do the outside people understand how things work and what their role should be–and if not, how can you fix it?

Success Isn't Always Good

When it comes to incident response simulations, everyone tries to win. They want to "beat" the problem and save the day. Which is good! That doesn't mean they should succeed.

The point of these simulations is to learn about your weaknesses. Scenarios should be challenging, and they should test every resource and idea you've got. Most scenarios should end in disaster.

In an ideal world, every practice would be a mess, and every real incident would be painless. And that's generally how it works. Response teams that never lose in a simulation are more likely to be overwhelmed when the reality check arrives. But you need to make sure people expect it, especially management. Treat it like the popular board game *Pandemic*. In *Pandemic*, players cooperate "against" the game, which is combating a global epidemic. The game rarely ends well for the players; playing the easiest rules with the best combination of roles, players succeed only about a third of the time.

Yet, the game is popular; the original version and its spinoffs have collectively won many awards and are consistently rated among the top ten board games of all time. Players expect to be challenged. And even when they lose, the result is an enjoyable experience of learning and sharing and strategizing with friends.

That should be your goal.

Find the Unexpected

It can be a challenge to keep things fresh and new. You can't expect people to do random incident response scenarios at midnight, but you can do things to both keep involvement high, a strong element of surprise, and not be too disruptive in the process.

- **Mix up the roles.** Instead of the same people always playing the same roles in exercises, make them shake it up by assigning roles randomly–or intentionally aiming to put people into areas they haven't considered.
- **Block people from participating.** In a real incident, people won't be available for a variety of reasons, yet there are always high-performing folks that we depend on in emergencies. So call them in for an exercise, and when they arrive, inform them they are on vacation and out of contact in this scenario. They can only watch the exercise–no talking, no texting, no help–just notes and your observations about their comfort levels as the incident proceeds without them. Then get their feedback on how things could be improved so that they're not so critical.
- **Add surprises.** Most organizations have no choice but to conduct regular fire drills, and as mentioned earlier, most of them aren't very effective. One way to solve that problem is to add surprises to the exercises–both to make the events more realistic and to encourage participation. Have people handing out gift cards or challenge coins to people who actively participate in the exercises–and have some of your participants become incapacitated and require assistance for the evacuation. Don't take that too far–just give a few

people a card to hand the safety wardens and their coworkers saying “as part of this exercise, the person carrying this card cannot walk. Get them to safety.” Don’t tell them how it should be handled; see how the Safety Teams respond.

2.7 Executive Review and Approval

No program can be successful without the approval of executive management. When it comes to Incident Response, gaining that approval is, in some ways, more difficult than incident response itself. If there wasn’t a serious incident during the review period, there’s no definite “proof” of your program’s success. If there was an incident, any review is going to take place with the benefit of hindsight–and that rarely makes an incident response look better. There are always missed opportunities that would have been “better” than what actually happened.

Suddenly measuring success by the number of binders labeled “Incident Response Plan” looks like it might have something going for it after all, right?

There are ways to work with this situation, though, without resorting to that kind of metric. First, because your program hasn’t been focused on end goals, your executives should already be familiar with the idea of creating an organizational culture that can handle incidents, rather than an incident response team. So you can talk about the metrics that really do matter–the ones you measure to track your program’s growth and success. In an organization accustomed to traditional approaches to incident response, that can be a difficult sell at first, but it’s worth the effort to make it stick.

Next, involve your executive leadership in the exercises you run. Not only do they need to be involved in real incidents, but bringing them into the room for the exercises demonstrates both your confidence in the program and, over time, a feel for the program's progress. It's easier to explain a program's success to people who already understand it, so make sure they get that perspective.

Finally, remind the executive leadership–and yourself–that building an effective incident response program does not have an end goal. Building this capability in your organization is not something you do to achieve a particular metric or comply with some specific regulation. Giving your team the ability and the opportunity to meet challenges and successfully operate through them has benefits that go far beyond any of that.

Consider Waffle House

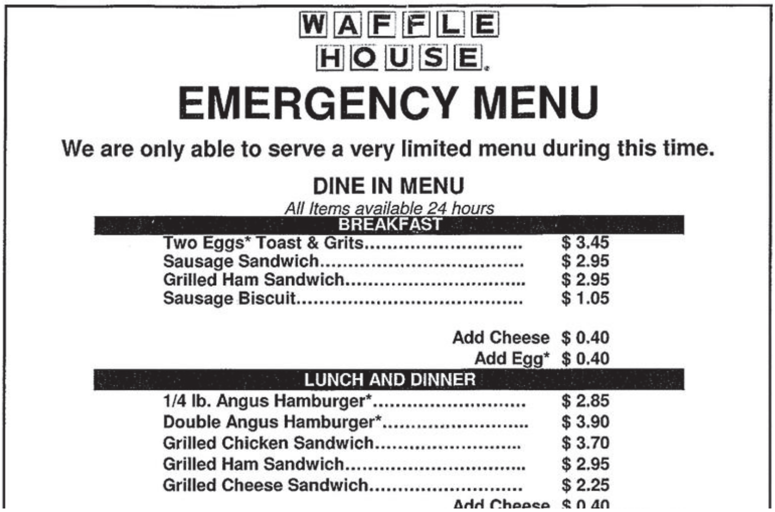
If you're not familiar, Waffle House is a large regional chain of restaurants, mostly in the southern United States. When you think "incident response" you might not automatically think of restaurants, but the fact is Waffle House has one of the most comprehensive–and effective–incident response programs anywhere. The chain has developed a reputation for staying open no matter what, to the point that emergency responders in national disasters use them as an ad-hoc measure of disaster impact.

If the Waffle House is closed, things are *really* bad.

That's not an accident. Waffle House made the policy decision that they would be open to serve whenever possible, including during natural disasters. They built priorities: menu items that would always be available, secondary items, and those they could easily do without; services and staff roles that would be essential in any situation and methods of ensuring their availability that people could depend on; and the development of "jump teams", built from groups throughout the entire organization, who could be moved to assist in emergencies when local staff might not be available.

They've built a program based on people and flexibility–create the possibility for success, then get out of the way and let the people on the ground make it happen. As Pat Warner, Waffle House's Director of Public Relations and External Affairs put it in a USA Today article: "We try to plan, and our plan gets us up to the storm. Once the storm hits, we really just react."[1]

Whether your goal is the invasion of Occupied Europe, or successfully serving breakfast foods, this is the best approach.



WAFFLE HOUSE

EMERGENCY MENU

We are only able to serve a very limited menu during this time.

DINE IN MENU

All Items available 24 hours

BREAKFAST	
Two Eggs* Toast & Grits	$ 3.45
Sausage Sandwich	$ 2.95
Grilled Ham Sandwich	$ 2.95
Sausage Biscuit	$ 1.05
Add Cheese	$ 0.40
Add Egg*	$ 0.40
LUNCH AND DINNER	
1/4 lb. Angus Hamburger*	$ 2.85
Double Angus Hamburger*	$ 3.90
Grilled Chicken Sandwich	$ 3.70
Grilled Ham Sandwich	$ 2.95
Grilled Cheese Sandwich	$ 2.25
Add Cheese	$ 0.40

Waffle House's emergency menu is designed for limited operation. No complex items, nothing requiring special equipment, and prices set to make math easy for tired staff and customers.[2]

[1] source: `https://www.usatoday.com/story/news/nation/2019/09/01/hurricane-dorian-waffle-house-index-disasters/2187708001/`

[2] source: `https://www.wabe.org/how-fema-uses-waffle-house-measure-disasters/`

3 Documentation and Process Management

An effective incident response program is based on people and culture. As we've discussed, that's a difficult thing to pin down with numbers and metrics. That means documentation, rigorous process management, and an effective culture of review and improvement are also requirements for regulatory compliance in incident response.

Any incident response audit will require artifacts of compliance. This *Minimum Viable Incident Response Program* does not require expensive tools, but there is a minimum set of documentation that can help satisfy audit requirements. Happily, the commonly required set for compliance and the essential structure for an effective program are very similar. The document set includes:

1. A formal Incident Response policy,
2. An Incident Response planning process,
3. Records of Incident Response exercises, reviews, and results,
4. Records of any actual incidents and after-action analysis and reports,
5. Completed Incident Response Plan(s) themselves,
6. Meeting minutes.

You'll need to adjust this to fit within your organizational culture and documentation structure, but keep in mind this is the *minimum* set. We'll address the purpose, contents, and utility of these elements below.

3.1 Incident Response Policy

The *Incident Response Policy* documents the intent and purpose of the incident response program. The documentation should include the purpose of the incident response program, its scope, priorities, and a statement highlighting the organization's compliance with applicable health and safety regulations.

The policy must also define how often plans will be reviewed, as well as the timing and cadence of regular reviews of the policy, process, and associated documents.

3.2 Incident Response Planning Process

The *Incident Response Planning Process* document supports the policy by providing details, procedural steps, and approval processes for creating and iterating incident response plans. It will identify the steps we've outlined above, as well as any necessary components, such as management approvals or required consultations with various departments or resources.

It's helpful to create and include a RACI matrix (Responsible, Accountable, Consulted, Informed) for the various roles involved in the incident response process. Example roles you should include are:

- **Incident Response Program Owner:** owns the program, n'est-ce pas?
- **Incident Response Coordinator:** creates, schedules, runs scenarios.
- **Incident Response Communications:** responsible for internal and external communications about the program and incidents.

- **General Counsel:** legal resource to assist in identifying regulatory or legal concerns.

3.3 Records of Incident Response Exercises, Reviews, and Results

The goal of these records is twofold–one, to demonstrate that you do have an active incident response program, including details of your program activities, and two, providing you with records and information to guide the growth and future activities of your program.

For every exercise, you need three documents:

1. Scenario

This document details the scenario you created for the exercise, including the people assigned to the scenario and notes of any important considerations–particularly the reasons the scenario was selected.

2. Scenario Results

What did the response team try? Did they identify any new resources or services that should be considered essential? Any particularly interesting points of discussion?

Notes from the exercise should focus on these points in particular. It's not very important to track the details of the scenario itself, but only the questions and concerns that come to light.

3. Action Items

Related to the Scenario Results, this details any actions the exercise generated for the organization. Those resources or services that got marked *critical* in the scenario? Figure out what needs to be done to mitigate that risk. Start projects, or request operational changes, or write new policies or procedures to address questions that couldn't be answered.

With these documents, you can not only demonstrate that your program is active and functional, but you can also look back and see what you've done and identify what you should do next.

3.4 Records of Incidents and After-Action Analysis and Reports

As with the exercises, so with any actual incidents your program encounters. For every exercise, you need three documents:

- Incident Description,
- Incident Results,
- Action Items.

Use the same document set and formats that you have for the exercises, but use records and interviews after the incidents to identify critical details, lessons for future incidents, and appropriate action items.

3.5 Completed Incident Response Plan(s)

Although plans are in and of themselves not very valuable, they are often required for various compliance criteria. Therefore, as your team creates them, they should be documented and stored to satisfy these requirements.

3.6 Meeting Minutes

One often overlooked compliance artifact is evidence that your program is active, maintained, and proceeding. The simplest method of demonstrating this is to document and retain *meeting minutes* for the proceedings of the incident response program. The minutes should track the purpose of each meeting, the date and time, attendees, items reviewed, and any decisions made.

3.7 Process Review

Incident response is a process, but the maintenance of that process is a program in itself. There is no final state, no end to planning incident response–unless the organization itself is dead.

Like any large-scale cultural program, your incident response program must change and adapt as your organization evolves and matures. You may find that a higher or lower frequency of test scenarios is needed, or that priorities have shifted over time. You might even need to completely rethink whole sections of the program from time to time.

A consistent and regular process review makes that easier and smoother for everyone involved.

The frequency of these reviews depends on the needs of the organization. The review requirements should be documented in the *Incident Response Policy*, with accompanying elements in the *Incident Response Process*. Regulatory frameworks may require annual or more frequent reviews, which should be included in your process planning. Whatever your chosen schedule, each review must evaluate the content and potential updates to all of the above documents (including the format of the *Meeting Minutes*).

4 Scaling, Growth, and Next Steps

A new incident response program should have a limited scope to make it manageable and increase the potential for program success. At some point, however, leadership will likely want to expand the scope as the success of the program makes the utility of incident response more obvious. When this happens, the program must scale up to meet the needs of the organization.

For the most part, this involves all the same activities, plans, and roles–but more of them. You'll need to include more people, broader representation from other parts of the organization, and even possibly change your priorities or approaches to different types of incidents.

The same approaches we've outlined should still work. And if not, they should at least give you the tools to identify that and look for new solutions to the challenges you find.

5 A Final Caveat

Think of this program as a scaffold: when the construction of your mature and robust Incident Response program is complete, there probably won't be a single piece of it left standing. Yet without the scaffolding, the project would have been much more difficult to accomplish.

6 Conclusion

Developing an effective incident response program is a challenging task. Most current guidance is based on the practices of large, mature organizations that can support expensive processes and tools for the sake of audit requirements. However, there is a real need to bring a solid incident response to smaller and less mature organizations that cannot afford the time or tooling required by the current guidance.

The measure of an incident response program is not whether the program passes an audit. That may be necessary, but it is the lowest possible bar–and far too many incident response programs do no more than that. The measure of an incident response program is the business value it brings. Are the processes aligned with business needs? Are people empowered and proactive when incidents occur? Can the organization function effectively through unexpected events and return to normal operations afterward? Do the results support business objectives?

The goal of this white paper is to give you a framework for implementing an effective Incident Response program. Like the program we describe, the documentation it calls for is not the goal. The important thing is your ability to think about incident response in a way that moves your organizational culture in the right direction.

◈◈◈

SMOOTH SAILING SOLUTIONS

The days when a “good enough” packaged solution could meet your needs are gone. Truly effective security and privacy programs must be integral to your business, a core component of company culture.

We work with your business across the board, combining the useful aspects of your new or existing solutions with policy and procedural changes that work within your company culture and infrastructure, rather than trying to bolt on to it or replace it.

It’s your company. Your strategy. Your vision. Our crew brings the knowledge, expertise, and experience to help you transform and get you where you want to go.

smoothsailingsolutions.com